SHEET 1 OF 5

## FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office

#### INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use several sheets if necessary)

ATTY.	DOCKET	NO
• • • •		

500.41092X00

SERIAL NO. 10/046,224

APPLICANT
M. NISHIOKA, et al

FILING DATE January 16, 2002 **GROUP** 2136

	<del></del>				<del>سر برید</del>					MENTS				FILING DAT	E
AMINER		DOCUM	ENT NU	ABER		_			DATE	NAME		CLASS	SUBCLASS	IF AFFRORN	<u> </u>
ITIAL		DOCOM						Ì							
						+									
	1					}									
	<b> </b>				1	1	İ								
	├										,				
												70	П		
		1		1						-56	<del>M</del>	D)/	W		
	+-	1									_]]]		<b>II</b>	<b> </b>	
	ļ	<b>_</b>	<b> </b> -									Ψ			
	1	<u> </u>					<b> </b>								
												<del> </del>			
	╌		-	<del>                                     </del>						Ĭ		\	<u> </u>	ļ	
			ļ	<del> </del>			<del> </del>	<del> </del> -							
	1		1				<u> </u>	<b>↓</b>	<b>}</b>			<del> </del>	<del>                                     </del>		
						ļ	Ì					<u>.l</u>			
					<u></u>		<u>,L</u>								
FORE	IGN	PATE	ENT	DOC	<u>UME</u>	NTS			T	T		CLASS	SUBCLASS	ABSTRACT	
		1		NUMBER					DATE	COUNTRY	Y	05.00		YES	N
	1									<del></del>			1		
	_					Į.	1	1	İ						-
	+		-}		-	†	1			-		\ _			<b> </b>
					┼	-}			+	+				}	
				ł											
		_	_												+-
	}-		+-		┼─	+		-				1			
						4_									
				1	1	1	1								

OTHER D	OCUMENTS (Including Author, Title) Date,
Rese	R. L. Rivest, et al "A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, vol. 21, No. 2. pp. 120-126, 1978.
262	V. S. Miller, Use of elliptic curves in Cryptography, Proc. of Crypto '85, LNCS218, Springer-Verlag, pp. 417-426, 1985.
dal	N. Koblitz, Elliptic Curve Crytosystems, Math. Comp. 48, 177, pp. 203-209, 1987.
EXAMINE	DATE CONSIDERED 1/3//2006

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

# SHEET 2 OF 5 SERIAL NO. ATTY, DOCKET NO. FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office 10/046,224 500.41092X00 INFORMATION DISCLOSURE **APPLICANT** STATEMENT BY APPLICANT M. NISHIOKA, et al **GROUP** FILING DATE (Use several sheets if necessary) 2136 January 16, 2002 U.S. PATENT DOCUMENTS FILING DATE SUBCLASS EXAMINER DATE DOCUMENT NUMBER INITIAL FOREIGN PATENT DOCUMENTS ABSTRACT SUBCLASS CLASS COUNTRY DATE DOCUMENT NUMBER YES NO OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.) M. O. Rabin, Digital Signatures and Public-key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCSTRANSMISSION-212, 1979. T. El Gamal, A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE, Trans. on Information Theory, IT-31, 4, pp. 469-472, 1985.

S. Goldwasser, et al Probabilistic Encryption, JCSS, 28, 2, pp. 270-299, 1984.

EXAMINER

DATE CONSIDERED

1/31/2606

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

	FORM F	e Pa INI ST	itent FORM ATE	and MATION	I rade I BY A	epartme mark C SCLOS APPLIC	URE ANT	n 4 7		ATTY. [ 500.4*  APPLIC M. NIS  FILING Januar	DATE ary 16, 2002			046,224 DUP	V 17 2005	
FOREIGN PATENT DOCUMENTS  DATE  DATE  NAME  SOLUTION  SOLUTION  SOLUTION  SOLUTION  FOREIGN PATENT DOCUMENTS  DATE  COUNTRY  CLASS  SUBCLASS  ABSTRACT  YES NO  NO  NO  NO  NO  NO  NO  NO  NO  NO		<b></b>					<u>U.S.</u>	PAT	ENI				T		FILING DATE	
FOREIGN PATENT DOCUMENTS  DOCUMENT NUMBER  DATE  COUNTRY  CLASS SUBCLASS  ABSTRACT  YES NO	EXAMINER		DOCU	IMENT N	UMBER					DATE	NAME	CLAS	s	SUBCLASS	IF APPROPRIA	TE
DOCUMENT NUMBER  DATE  COUNTRY  YES  NO	INITIAL												-+			
DOCUMENT NUMBER  DATE  COUNTRY  YES  NO												_	-+			
DOCUMENT NUMBER  DATE  COUNTRY  YES  NO		$\vdash$		1-	1								}-			
DOCUMENT NUMBER  DATE  COUNTRY  YES  NO		╁─╴	-	<del> </del>	_	1							=	JI		
DOCUMENT NUMBER  DATE  COUNTRY  YES  NO		-	┼	+-		1					~6	$I/\mathcal{L}$	24	71-		
DOCUMENT NUMBER  DATE  COUNTRY  YES  NO		╁		╁┈		1										
DOCUMENT NUMBER  DATE  COUNTRY  YES  NO			-		+			-			9					
DOCUMENT NUMBER  DATE  COUNTRY  YES  NO			┼	-												
DOCUMENT NUMBER  DATE  COUNTRY  YES  NO			-					<del></del>								
DOCUMENT NUMBER  DATE  COUNTRY  YES  NO			-													
DOCUMENT NUMBER  DATE  COUNTRY  YES  NO												_				
DOCUMENT NUMBER  DATE  COUNTRY  YES  NO		<u> </u>									1			<u> </u>		
DOCUMENT NUMBER  DATE  COUNTRY  YES  NO	FORE	IGN	PAT	ENT	DO	CUME	NTS				T			CURCLASS	ABSTRACT	
										DATE	COUNTRY	۲	LASS	SUBCLASS		NO
							<del></del>	<u> </u>								
						_	<del> </del>				<del> </del>					
								<b></b>						<del> </del>		
																<u> </u>

		1	Ì						<u> </u>								
							A4la	_ T	Title Date P	ertin	ent P	ages	, Etc	:.)			
OTHER	DO	CUM	<u>ENT</u>	S (In	clud	ing /	Auth	or, i	Title, Date, P	<u> </u>				الما مامامات	idoc	all Pa	rtial
080							_		listic Public-ke NCS196, Spring	w Enr	WINTIN	ın acıı	BIIIE	44 1 1 1 C 1 1		anra	
000		Info	rmati	on, P	roc. C	JI CIY	<u> </u>	<del>,</del>			h44m·ha	OTOM-C	SA.				
000		1	4 -4.	ducal	~e/mil	hir/19:	97.		s on Cryptogra								
	┼	ucs	<u>u</u>				Dubl	ie ko	y Cryptosyster	m as S	Secure	e as Fa	actor	ing,  Pro	c. of	Euro	crypt
260		T. C	kame LNC	oto, e S1 <u>40</u> 3	it al, / 3, Spi	new ringer	Veri:	ag, p	p. 308-318, 199	98.							
EXAMIN	FR	1		2	4		DA	TE C	ONSIDERED	1/	1311	5 @	06				

EXAMINER: Initial if citation is considered, draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

(Form PTO-1449 [6-4])

SHEET 4 OF 5

ATTY. DOCKET NO.

500.41092X00

NOV 1 7 2005 SERIAL FRARE 10/046,224

## FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office

### INFORMATION DISCLOSURE STATEMENT BY APPLICANT

APPLICANT
M. NISHIOKA, et al

FILING DATE

GROUP

		(Use s	everal	sheets	If nec	essaı	ry)			FILING Janua	DATE ry 16,	2002		2136			
<del></del>							บ.ร	. PA	TEN	DOCU	MENT	rs	<del></del>	<del>,                                    </del>			
CAMINER	<u> </u>	DOCUMENT NUMBER								DATE		NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE		
ITIAL	-	DOC	JMENT N	UMBER	T	$\top$								<b> </b>			
	┼	-	+	-	+	1											
	-	-	┼	+	+-	+											
<del></del>	<del> </del>		+-	-	+-									D/(C			
		-		-	-	+											
				-	-	-+											
						_							+				
											<del> </del>			<del> </del>			
	1										<u> </u>				<u> </u>		
FORE	L L	DAT	ENT	DO	CUN	ΛΕΝ	NTS								T		
FORE	IGN		CUMEN'							DATE	1	COUNTRY	CLASS	SUBCLASS	ABSTRACT YES	NO	
		"	COMEN							\ \					1 163		
	_									<u> </u>	<del> </del>					<del>                                     </del>	
	-	+	_						<u> </u>		<u> </u>						
	-	-	_	+	_					Ţ							
					+		<del>                                     </del>									├	
					-+		-	+-	1								
					}		┼	┿	+-							<u> </u>	
							<u> </u>						<del></del>	Etc \			
OTH	ER (	oc	UME	NTS	(In	clu	ding	Aut	hor,	Title, D	ate, P	ertinent (	ages,	Lto.)	Theory of		
0/0	0	- 1	n Do	IVA. e	t al	Non	-Mall	eable	Cryp	tography	y, In 23'	<sup>rd</sup> Annual A	ACM Syr	nposium on	Theory of		
124			Com	outing	<u>, pp</u>	. 54	2-552	2, 199	1			· Coouro A	nainst C	hosen Ciph	ertext Atta	cks,	
De	9		M. Na Proc	or, e	t at F	ubl , AC	ic-ke M Pr	y Cry ess,	ptosy pp. 42	stems P 27-437, 19	990.	- Secure A		hosen Ciph	oc. of Euro		
Dal	2					. 1 11/	\_4im	al As	ymm ag, p	etric Enc p. 92-111	ryption , 1994.			rith RSA, Pro			
EXA			20		6	4	<del></del>	\ C	ATE (	CONSIDE	ERED	1 (.	31/2			<del></del>	
EVA	MINE	:R· 1	nitial	if cita	tion	is c	onsi	derec	l, drav	v line thr	ough c	itation if n	ot in cor ant.	nformance a	na not		
COUS	ider	ed.	nclud	e cop	y of	this	form	n witl	n next	commu	mication	n to application of the property of the proper	49 [6-4])				

### FORM PTO-1449 U.S. Department of Commerce Patent and Trademark Office

#### INFORMATION DISCLOSURE STATEMENT BY APPLICANT

SERIAL NO.
10/046,224

•							<u> </u>						
	(Use se	veral sh	eets if n	ecessa	ry) 			FILING Janu	DATE ary 16, 2002		GROUP 2136		
					U.S	. PAT	ENT	DOC	JMENTS	_			<del></del>
AMINER								DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE	
TIAL	DOCUM	ENT NUM	BER		T	$\overline{}$		ZA 1 E					
	╂				_								
										1			_
	<del>-</del>									<del>-  </del>			
											10/		
				_+	}				6	5	THE STATES		
									<del> ((-</del>		111	<del> </del>	
										4		-	
											<del></del>	<del> </del>	-
OREIGN	PATE	NT D	OCU	IMEN	ITS							<del></del>	
OKLIGIA		MENT NU						DATE	COUNTRY	CLA	SS SUBCLASS	ABSTRAC	T
			<del></del>	<del></del>		<del></del>			<del> </del>			YES	NO NO
													+
													╂
													<del></del>
	_												
	_	<del>                                     </del>											
					ling	Auth	or Til	le. D	ate, Pertinent I	ages,	Etc.)		
	1							•	- 4 4 Drava	nlw Sar	ura Adainst A	daptive	
We!	- L Ch	กลลดา	Ciphe	rtext	Attac	:K, Pro	C. OI C	Typto	90, LIVOU (402) 0	F9 **			<u>8.</u>
00		D-11-		al Bal	ation	e Amo	na No	tions	of Security for Pu	blic-ke	y Encryption	Schemes	, Pro
ne	of	Crypt	o <sup>'</sup> 98,	LNCS	<u> </u>	2, Spri	nger V	erlag,	pp. 26-45, 1998.				
										1 ,			
EXAMINE	11-1		C		)—	<u>.l</u> .	TE COI				2006		
EYAMINE	R: Initi	al if ci	tation	is co	nside	ered, d	iraw lir	ne thro	ough citation if no	t in co	nformance an	d not	
considere	d. Incl	ude co	opy of	this 1	form	with n	ext co	mmun	ication to applica				

(Form PTO-1449 [6-4])